Ministério da Educação - MEC
Secretaria de Educação Profissional e Tecnológica (SETEC)
Instituto Federal de Educação, Ciência e Tecnologia do Ceará

INSTALADOR E REPARADOR DE REDES DE COMPUTADORES

CABEAMENTO ESTRUTURADO E REDES DE ACESSO

INSTALAÇÕES DE REDES LOCAIS

SAULO DE LIMA BEZERRA

FIC

CRÉDITOS

Presidente
Dilma Vana Rousseff

Ministro da Educação
José Henrique Paim Fernandes

Secretaria de Educação Profissional e Tecnológica
Marco Antonio de Oliveira

Reitor do IFCE
Virgílio Augusto Sales Araripe

Pró-Reitora de Extensão
Zandra Maria Ribeiro Mendes Dumaresq

Pró-Reitor de Ensino
Reuber Saraiva de Santiago

Pró-Reitor de Administração
Tássio Lofti

Coordenador Geral
Jose Wally Mendonça Menezes

Elaboração do conteúdo
SAULO DE LIMA BEZERRA

Coordenador Adjunto Campus
André Luiz da Cunha Lopes

Supervisor(es) Curso(s)
José Tavares de Luna Neto

Orientador(es) Curso(s)
José Willame Felipe Alves

Equipe 1
APOIO ADMINISTRATIVO ACADÊMICO

APOIO ADMINISTRATIVO FINANCEIRO

Francisco Gomes de Loiola Neto

O QUE É O PRONATEC?

Criado no dia 26 de Outubro de 2011 com a sanção da Lei nº 12.513/2011 pela Presidenta Dilma Rousseff, o Programa Nacional de Acesso ao Ensino Técnico e Emprego (Pronatec) tem como objetivo principal expandir, interiorizar e democratizar a oferta de cursos de Educação Profissional e Tecnológica (EPT) para a população brasileira. Para tanto, prevê uma série de subprogramas, projetos e ações de assistência técnica e financeira que juntos oferecerão oito milhões de vagas a brasileiros de diferentes perfis nos próximos quatro anos. Os destaques do Pronatec são:

- Criação da Bolsa-Formação;
- Criação do FIES Técnico;
- Consolidação da Rede e-Tec Brasil;
- Fomento às redes estaduais de EPT por intermédio do Brasil Profissionalizado;
- Expansão da Rede Federal de Educação Profissional Tecnológica (EPT).

A principal novidade do Pronatec é a criação da Bolsa-Formação, que permitirá a oferta de vagas em cursos técnicos e de Formação Inicial e Continuada (FIC), também conhecidos como cursos de qualificação. Oferecidos gratuitamente a trabalhadores, estudantes e pessoas em vulnerabilidade social, esses cursos presenciais serão realizados pela Rede Federal de Educação Profissional, Científica e Tecnológica, por escolas estaduais de EPT e por unidades de serviços nacionais de aprendizagem como o SENAC e o SENAI.

Objetivos

- Expandir, interiorizar e democratizar a oferta de cursos de Educação Profissional Técnica de nível médio e de cursos e programas de formação inicial e continuada de trabalhadores;
- Fomentar e apoiar a expansão da rede física de atendimento da Educação Profissional e Tecnológica;
- Contribuir para a melhoria da qualidade do Ensino Médio Público, por meio da Educação Profissional;
- Ampliar as oportunidades educacionais dos trabalhadores por meio do incremento da formação profissional.

Ações

- Ampliação de vagas e expansão da Rede Federal de Educação Profissional e Tecnológica;
- Fomento à ampliação de vagas e à expansão das redes estaduais de Educação Profissional;
- Incentivo à ampliação de vagas e à expansão da rede física de atendimento dos Serviços Nacionais de Aprendizagem;
- Oferta de Bolsa-Formação, nas modalidades:
- Bolsa-Formação Estudante;

- Bolsa-Formação Trabalhador.
- Atendimento a beneficiários do Seguro-Desemprego;

SUMARIO

Rede de computadores

Inicialmente, os computadores eram máquinas caríssimas que centralizavam em um único ponto o processamento das aplicações de vários usuários, e muitas vezes, de toda uma organização. Com a redução de custos do hardware e a introdução dos microcomputadores no cenário da informática, a estrutura centralizada cedeu lugar a uma estrutura totalmente distribuída, na qual, diversos equipamentos dos mais variados portes, processam informações de formas isoladas, o que acarreta uma série de problemas. Dentre eles destaca-se a duplicação desnecessária de recursos de hardware (impressoras, discos, etc.) e de software (programas, arquivos de dados, etc.).

Sistema de Comunicação

Nesse cenário, surgiram as redes de computadores, onde um sistema de comunicação foi introduzido para interligar os equipamentos de processamentos de dados (estações de trabalhos), antes operando isoladamente com o objetivo de permitir o compartilhamento de recursos, ou seja, uma rede. Uma rede é um grupo de pelo menos dois computadores que são ligados entre si de forma que possam se comunicar uns com os outros, compartilhando recursos e informações com maior velocidade e praticidade.

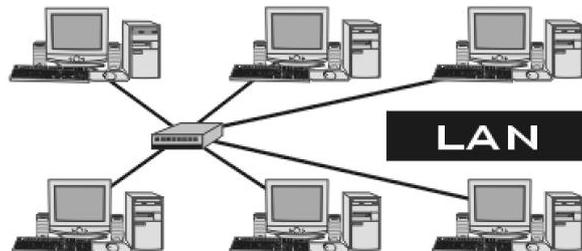
A maioria das redes é baseada em alguma espécie de cabo utilizado para ligar os computadores entre si, além do cabo, é necessária outra peça física para fazer a conexão entre os computadores, este equipamento é chamado de placa de interface de rede (NIC), ou simplesmente placa de rede.

Rede local – (Local Área Network)

Surgiram dos ambientes de institutos de pesquisa e universidades, o enfoque dos sistemas de computação que ocorriam durante a década de 1970 levava em direção à distribuição do poder computacional. Redes locais surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), preservando a independência das várias estações de processamento, e permitindo a integração em ambientes de trabalho cooperativo. Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região, na maioria das vezes pertencente a uma mesma entidade ou empresa,

como, por exemplo, um escritório, um prédio ou um complexo de prédio de uma empresa. O número de computadores é limitado e geralmente interligado por cabos.

Outras características típicas encontradas e comumente associadas às redes locais são: altas taxas de transmissão e baixas taxas de erro; outra característica é que em geral elas são de propriedade privada.

LAN

Rede pessoal – (PAN - Personal Area Network)

É formada por nós muito próximo uns dos outros, normalmente a distância não passa de uma dezena de metros.

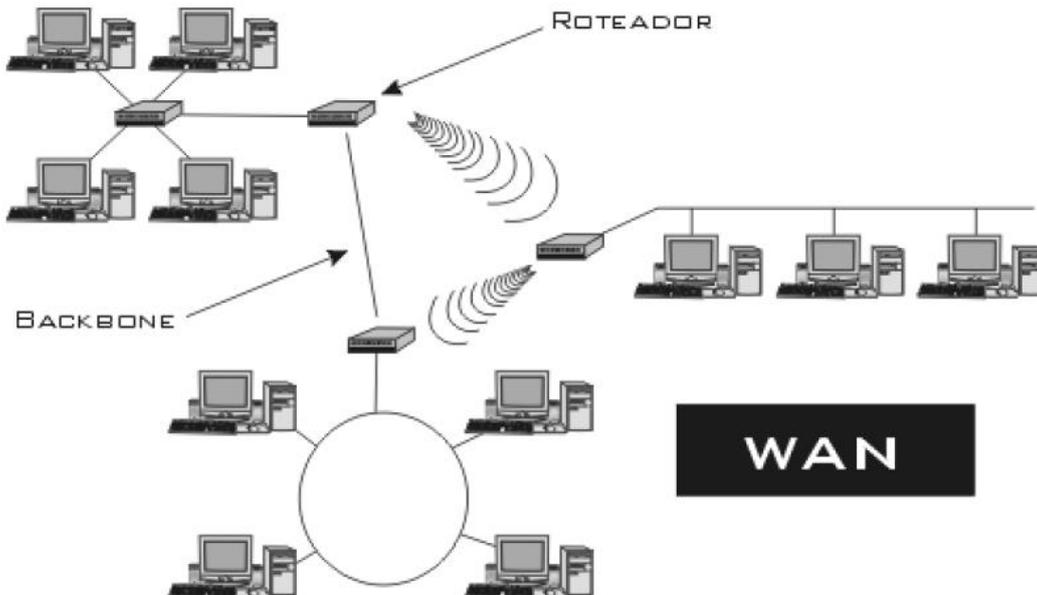
São um exemplo de PAN as redes do tipo Bluetooth.

Rede metropolitana – (MAN - Metropolitan Area Network)

São redes que ocupam o perímetro de um bairro ou uma cidade.

Permitem que empresas com filiais em bairros diferentes se comuniquem entre si.

Redes geograficamente distribuídas (WAN – Wide Área Network)

Surgiu da necessidade de se compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos. Por terem um custo de comunicação bastante elevado (circuitos para satélites e enlaces de microondas), tais redes são em geral públicas, isto é, o sistema de comunicação, chamado sub-rede de comunicação, é mantido, gerenciado e de propriedade pública. Em face de várias considerações em relação ao custo, a interligação entre os diversos módulos processadores em uma tal rede determinará a utilização de um arranjo topológico específico, diferente daqueles utilizados em redes locais. Ainda por problemas de custo, as velocidades de transmissão empregadas são baixas: da ordem de algumas dezenas de kilobits/segundo (embora alguns enlaces cheguem hoje a velocidade de megabits/segundo). Por questão de confiabilidade, caminhos alternativos devem ser oferecidos de forma a interligar os diversos módulos.

A conexão de todas essas redes, locais, metropolitanas e geograficamente distribuídas, é o que chamamos de Internet.

O enfoque deste curso é voltado para as bases de arquitetura de rede e a tecnologia em um ambiente local, mas faz referência às necessidades das empresas de redes empresariais (Enterprise Wide Network).

Arquiteturas de Redes

No mundo da informática, existem alguns problemas em que as pessoas são tão divididas que os debates adquirem o caráter de discussões religiosas, acredite, você já ouviu uma discussão entre um usuário de PC e um usuário de Mac?

Até agora, o debate Ponto a Ponto versos Cliente/Servidor não chegou a esse estágio, mas existem pessoas que realmente acreditam em um ou outro, às vezes sem qualquer razão para isso, a não ser que um arranjo (Ponto a Ponto ou Cliente/Servidor) foi o primeiro a ser apresentado.

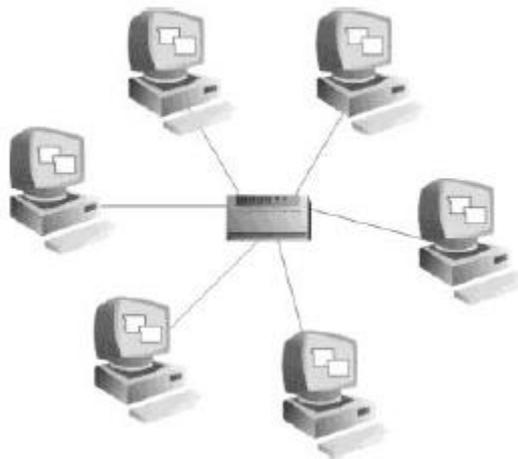
Nenhuma das duas arquiteturas é perfeita para todas as situações. As redes Cliente/Servidor têm melhor segurança, enquanto as redes Ponto a Ponto são mais flexíveis e freqüentemente mais baratas. A principal razão disso é o fato de que as redes Cliente/Servidor exigem uma pessoa que seja treinada especificamente e conheça bem o sistema operacional de rede Cliente/Servidor. As redes Ponto a Ponto não exigem tanto treinamento para operá-las.

Ponto-a-ponto (Workgroup)

A rede ponto-a-ponto também é chamada de não hierárquica ou homogênea, pois parte-se do princípio de que todos os computadores podem ser iguais, sem a necessidade de um micro

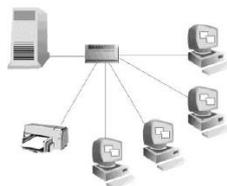
que gerencie os recursos de forma centralizada. O usuário pode acessar qualquer informação que esteja em qualquer um dos computadores da rede sem a necessidade de pedir permissão a um administrador de rede.

Neste tipo de rede o próprio sistema operacional possui mecanismos de compartilhamento e mapeamento de arquivos e impressoras, mecanismos de segurança menos eficientes, esta arquitetura é indicada para redes com poucos computadores.

As redes ponto-a-ponto são utilizadas tanto em pequenas empresas como em grupos de trabalho ou departamentos.

Características:

- Utiliza sistema operacional do tipo local
- Possui limite de máquinas
- Possui limite de acessos
- Segurança limitada
- Mais barata

Cliente/Servidor

A arquitetura Cliente/Servidor é mais sofisticada, nesta arquitetura o usuário fica dependente do Servidor, uma máquina central, que retém todas as leis de utilização da rede em um software chamado Sistema Operacional de Rede (NOS).

Para instalação, configuração e gerenciamento mais complexo, será necessário ter um profissional habilitado para a função de administrar desta rede.

Características:

- Utiliza sistemas operacionais locais e de rede
- Não possui limite de máquinas
- Gerência o acesso aos recursos
- Muita segurança
- Mais cara

Topologias

A topologia refere-se à disposição dos componentes físicos e ao meio de conexão dos dispositivos na rede, ou seja, como estes estão conectados.

A topologia de uma rede depende do projeto das operações, da confiabilidade e do seu custo operacional.

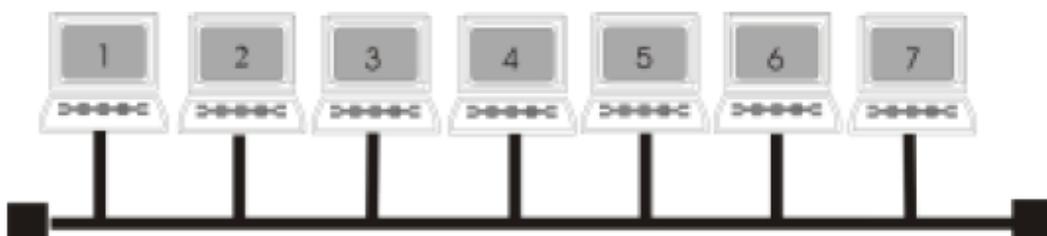
Ao se projetar uma rede, muitos fatores devem ser considerados, mas a topologia a ser empregada é de total importância para o bom desempenho e retorno do investimento de uma rede.

Cada topologia possui suas características, com diferentes implicações quanto ao desenvolvimento, operação e manutenção da rede, além disso, cada topologia apresenta duas formas, a forma física e a lógica. A topologia em sua forma física identifica como os nós estão interconectados uns nos outros.

Várias são as formas de interligação, embora as variações sempre derivem de três modelos básicos, que são as mais freqüentemente empregadas, barramentos, anéis e estrelas.

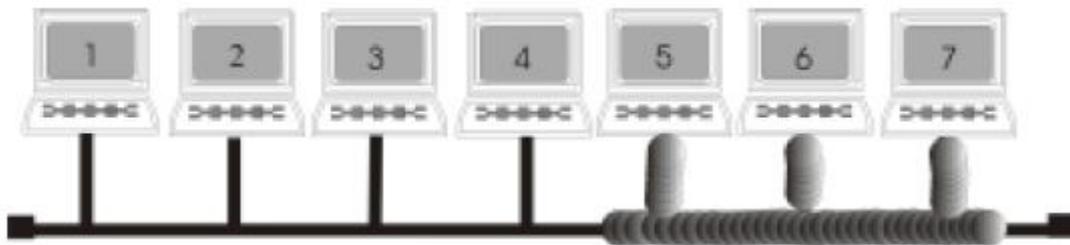
A topologia em sua forma lógica tem o papel de descrever um esquema usado pelo sistema operacional da rede, para administrar o fluxo de informações entre os nós rede. A maioria dos sistemas operacionais de redes utiliza-se de duas principais topologias lógicas, a Linear e a Token Ring.

Barramento

- Topologia física

É a topologia mais fácil de instalar. Nas redes de topologia barramento cada nó é conectado a um único cabo (espinha dorsal), porém esta estrutura deve completar-se em ambas as pontas com um conector especial chamado Terminador.

O desempenho de um sistema em barra comum é determinado pelo meio de transmissão, número de nós conectados, controle de acesso, tipo de tráfego entre outros fatores.

Esta rede utiliza o cabo coaxial e o padrão de comunicação Ethernet.

- Topologia lógica

Cada nó na barra pode ouvir todas as informações transmitidas. Esta característica facilita as aplicações com mensagens do tipo difusão (para múltiplas estações). Existe uma variedade de mecanismos para o controle de acesso à barra, que pode ser centralizado ou descentralizado. A técnica adotada para acesso à rede é a multiplexação no tempo. Em controle centralizado, o direito de acesso é determinado por uma estação especial da rede, o Servidor. Em um ambiente de controle descentralizado, a responsabilidade de acesso é distribuída entre todos os nós.

Vantagens

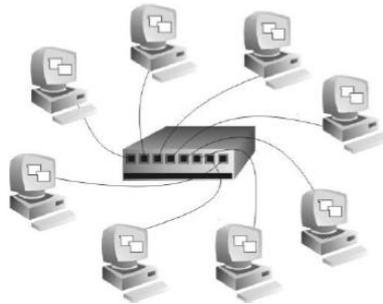
- Muita facilidade na instalação
- Baixo Custo
- Requer menos cabos

Desvantagens

- No caso de ter problemas de transmissão, é difícil isolar a causa, já que todos os nós estão conectados ao mesmo meio físico.
- Se o cabo danificar ou a ponta romper, os nós não poderão comunicar-se e a rede deixará de funcionar.
- A rede fica mais lenta em períodos de uso intenso.
- Excesso de colisões

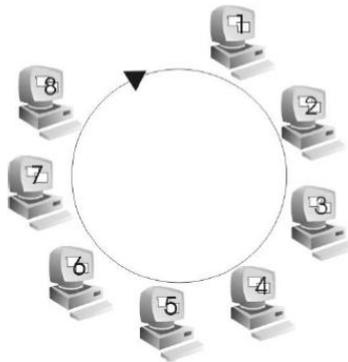
Anel

- Topologia física

Essa topologia é muito parecida com a topologia Estrela, porém seu funcionamento lógico é completamente diferente.

Os maiores problemas desta topologia são relativos à sua pouca tolerância a falhas.

Este modelo de topologia utiliza um HUB que internamente possui um anel que faz a busca dos computadores

- Topologia lógica

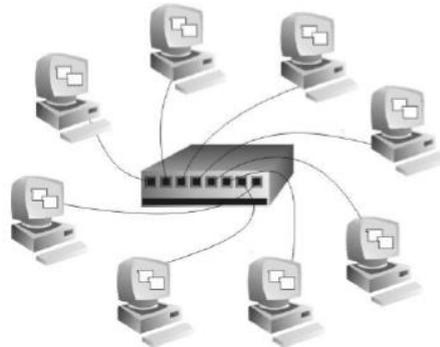
Abaixo temos uma ilustração do funcionamento, é importante lembrar que este movimento de anel é feito internamente no HUB.

Vantagens

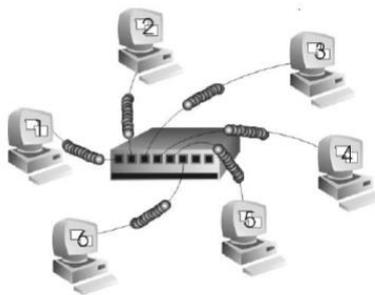
- Fácil adição e remoção de estações

Desvantagens

- Mais cara
- Muito complexa de instalar.
- Pouco conhecida

Estrela

- Topologia física

Em uma topologia física estrela todos os dispositivos da rede são conectados a um dispositivo central, este pode ser um computador Mainframe, um dispositivo comutador PBX, ou mais comumente, em dispositivos LAN's atuais, um HUB ou concentrador.

- Topologia lógica

A topologia lógica tipo estrela é comum em ambiente de rede de grande porte, ou em ambiente de rede utilizando PBX como um dispositivo comutador central de dados. Nos ambientes LAN mais comuns, a estrela é implementada como física e não como uma topologia lógica.

Este modelo de topologia utiliza-se do padrão de comunicação Ethernet e do padrão de comunicação ArcNet, Ethernet quando se utiliza de cabo par trançado e ArcNet quando se utiliza de cabo coaxial.

Vantagens

- Gerenciamento Centralizado
- A adição de estações é feita conectando-se as mesmas às portas de comunicação que estejam livres.
- A análise de problemas na rede é feita de maneira mais simples.
- Uma máquina ou cabo defeituoso não afeta o restante da rede.

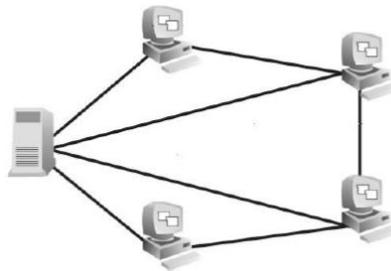
Desvantagens

- O número de estações fica limitado ao número de portas do HUB / Switch.
- Utiliza uma quantidade maior de cabos tendo em vista que cada estação deverá ter seu próprio cabo para conexão ao dispositivo central, elevando o custo da rede.

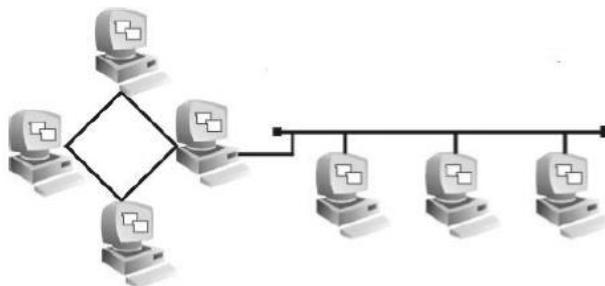
Outras topologias

Encadeada

Esta topologia parece em cruzamento entre as topologias de barramento e anel, isto é, cada nó é conectado diretamente a outros dois por seguimento de cabo, mas os seguimentos formam uma linha e não um anel e o sistema operacional passa as informações para cima e para baixo na cadeia até alcançar o endereço desejado.

Grafo (Parcial)

Este modelo de topologia engloba características de várias topologias. Cada ponto da rede possui uma rota alternativa para caso de congestionamento ou falha. As rotas são definidas por máquinas que tem a função de rotear endereços que não pertence a sua rede.

Híbrida

Uma topologia híbrida é uma combinação de barramento e anel, utilizado quando temos a necessidade de interligar duas ou mais redes de diferentes topologias.

Árvore

Uma topologia Árvore é utilizada principalmente na ligação de Hub's e repetidores, conhecida também por cascateamento.

Padrões de comunicação

Muitos e importantes padrões LAN têm evoluído, desde o início dos anos 80, conduzidos pelo Institute of Electrical and Electronics Engineers (IEEE) e o American National Standards Institute (ANSI). Este curso irá focalizar os mais conhecidos padrões LAN:

Ethernet

Nos finais da década de 60, a Universidade de Hawai desenvolveu uma WAN (Wide Area Network) chamada ALOHA utilizando o CSMA/CD como método de acesso ao meio. Poderíamos dizer que este foi o início do padrão Ethernet.

Na década de 70, o consórcio de empresas formado pela Intel, Xerox e DEC, desenvolveu o padrão Ethernet, o qual abrange a camada física e camada de link de dados do modelo OSI.

Esta especificação permite uma interconexão eficiente de equipamentos e também a sua implantação a um custo moderado. Esta especificação considera a camada física do modelo OSI e divide a camada de link em duas partes :

- Controle de Acesso
- Controle de Enlace

A Camada física se encarrega de prover os serviços de transmissão e recepção de dados, definindo as características: Elétricas, níveis de tensão e impedância, Mecânicas, tipo de conector e tipo de cabo e funcionais, tempo de duração do dado e velocidade de transferência.

Sub-Camada de controle de acesso ao meio arbitra o compartilhamento do meio de transmissão comum aos usuários da rede.

A subcamada de controle de enlace se encarrega de garantir uma comunicação confiável entre os usuários.

O padrão Ethernet trafega os dados em forma de pacotes chamados frames. O tamanho do frame em uma rede Ethernet pode estar entre 64 e 1.518 bytes, dos quais, 18 bytes são de controle.

Componentes Físicos de uma Rede

Placa adaptadora de rede (NIC)

Este periférico é o componente mais importante da estação de trabalho da rede. Seu objetivo principal é enviar os dados através da rede e receber aqueles enviados para a estação de trabalho.

Embora diversos fabricantes produzam placas de rede, todas elas podem ser usadas para falar com as outras em qualquer sistema de rede. O mais importante ponto de compatibilidade é o tipo de barramento na estação de trabalho no qual elas estão sendo instaladas.

Você não pode adquirir uma placa de barramento PCI quando na estação de trabalho só existe barramento ISA.

Também não pode se esquecer de conferir se a placa que esta sendo adquirida possui suporte para o cabeamento de sua rede.

Cada placa é fabricada com um único e permanente endereço eletrônico. Os fabricantes licenciam blocos de endereços para fabricarem suas placas e, salvo algum erro notório por parte do fabricante, este sistema de licenciamento garante que nunca haverá duas placas com o mesmo endereço. Este endereço é um código hexadecimal de doze dígitos, que limita a quantidade de endereços disponíveis em aproximadamente 70 trilhões. Os fabricantes não conseguiram esgotar os endereços tão cedo.

Além do endereço eletrônico as placas de rede possuem, ainda, duas importantes variáveis que ditam o comportamento de uma placa, são eles: o endereço de porta e a interrupção.

O endereço de porta é diferente do endereço permanente da placa. Enquanto o endereço permanente identifica a placa em toda a rede, o endereço de porta é um número usado pela estação de trabalho para selecionar um circuito eletrônico local para o qual ele direciona os dados de chegada e de saída da placa. Um endereço de porta comum é 300h.

A estação de trabalho deve ser configurada para enviar os dados da rede para o endereço de porta correto e a placa deve ser configurada para reconhecer quando os dados são enviados para esse endereço. Se as configurações do hardware não estiverem de acordo, os dados serão enviados para qualquer outro lugar (para impressora, mouse ou qualquer outro), a rede não conseguirá responder e a estação de trabalho poderá simplesmente travar.

HUBS

Hubs são dispositivos usados para conectar os equipamentos que compõem uma LAN. Com o Hub as conexões da rede são concentradas (daí um outro nome para Hub que é Concentrador), ficando cada equipamento em um próprio segmento.

O gerenciamento da Rede é facilitado e a solução de problemas também, uma vez que se existir um defeito, este fica isolado no segmento da Rede. Um exemplo comum de Hub é o hub Ethernet com 10Base-T (conectores RJ-45) e às vezes são parte integrante dos Bridges e Roteadores.

Ele controla a Rede em função da programação recebida do servidor que a ele estiver conectado. Assim, podemos definir ramificações da rede com horários específicos de utilização, entre outras coisas. A utilização dos Hubs é muito interessante por outros motivos, tais como:

O servidor trabalhará mais "folgadamente" e esta folga quer dizer aumento da produtividade e desempenho.

A Rede ficará mais segura. Por exemplo, se em uma grande Rede, com ligação em Estrela um dos cabos se partir, somente a ramificação desse cabo defeituoso deixa de funcionar.

A cada entrada do Hub podemos conectar qualquer dispositivo de rede local, e com isso pode-se aumentar a extensão (tamanho) da Rede, conforme seja necessário, e a distribuição da Rede pode ser mais bem equilibrada.

Os Hubs precisam ter características que permitam proteção contra intrusão e proteção contra interceptações, e também características de empilhamento e gerenciamento. Proteção contra Intrusão quer dizer que, em cada porta do Hub, só será permitidos a ligação de microcomputadores com endereço físico de Rede que estiver configurado para a porta do equipamento, e proteção contra Interceptação, quer dizer, que um dado transmitido só será reconhecido e válido na porta configurada com endereço da rede que coincide com o da mensagem, e nas outras portas a mensagem não é válida.

Em um Hub são centralizados os fios de ligação das diferentes estações (workstation). O Hub se encarrega de distribuir os sinais elétricos entre os vários equipamentos que compõem a rede, isolando os problemas de cada uma das estações e garantindo maior nível de segurança e confiabilidade ao sistema.

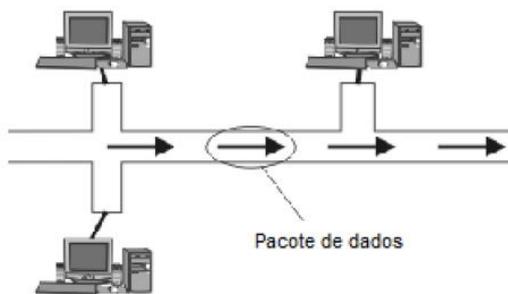
Hubs Passivos

São pequenas caixas, que têm apenas um conjunto pequeno de portas para a ligação de estações de computadores em topologia estrela. Um Hub Passivo pode ser também um painel de fios. Nesse tipo de Hub não existe amplificação dos sinais. Um hub passivo é resumidamente uma caixa de junção que não precisa de ligação elétrica, ou seja, é um simples repetidor.

Hubs Ativos

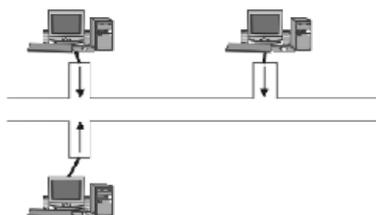
Normalmente possui mais portas que os hubs passivos e regeneram ativamente os sinais de um dispositivo para outro. Requerem ligação elétrica. Os Hubs Ativos são usados como repetidores para proporcionar uma extensão do cabo que liga as estações de trabalho.

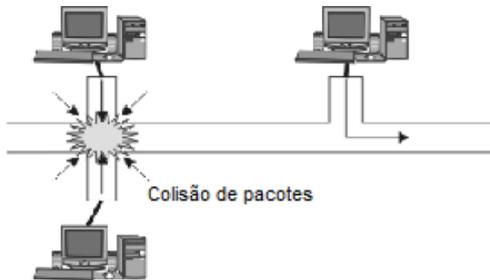
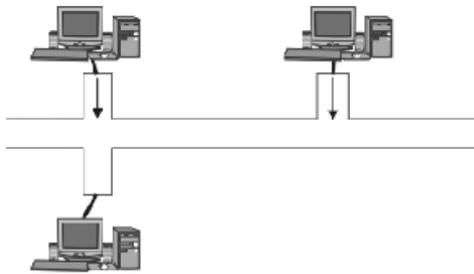
- CS (Carrier Sense) - Sensor mensageiro

Pacote de dados

Significa que sempre que um computador quiser enviar uma mensagem pelo cabo da rede, ele primeiro vai "ouvi-lo" para saber se alguém mais enviou uma mensagem, ou seja, irá verificar se outra estação está transmitindo no cabo, o computador pressupõe que esteja livre para enviar a sua, ou seja, a placa de rede do computador só irá transmitir a mensagem quando o cabo estiver livre.

- MA (Multiple Access) – Acesso múltiplo

Significa que não existe nada que impeça que dois ou mais computadores tentem enviar uma mensagem ao mesmo tempo. O Carrier sense verifica se algum computador está enviando mensagem e espera que o tráfego fique livre. Mas, e se os outros computadores

estiverem fazendo a verificação ao mesmo tempo, e decidirem enviar dados ao mesmo tempo? É o mesmo que um cruzamento em que os dois semáforos indiquem a cor verde para os carros passarem.

- CD (Collision Detection) – Detecção de colisões

Significa que depois que a placa adaptadora envia uma mensagem na rede, ela verifica atentamente para ver se colidiu com outros dados na rede.

Se uma colisão foi detectada, as placas adaptadoras de rede começam a transmitir um sinal especial, garantindo que todos os nós conflitantes percebam a colisão. As placas adaptadoras podem detectar essas colisões por causa do nível do sinal elétrico mais alto que as transmissões simultâneas produzem. Em seguida, todas as placas param de transmitir e cada uma determina um tempo de espera aleatório para poder transmitir novamente. Como o tempo de espera é aleatório, dois envios de dados que colidiram serão retransmitidos depois de diferentes tempos de espera, portanto uma segunda colisão é improvável.

O aumento da quantidade de estações provocará uma intensa solicitação na rede, aumentando a probabilidade de colisões, o que provoca a diminuição de velocidade de comunicação. A vantagem do CSMA/CD é que cada estação sempre irá transmitir quando estiver pronta, independente das outras, o que o torna bastante simples e não cria nenhum overhead (sobrecarga).

Switch

É um componente utilizado para conectar segmentos de redes locais. Ele envia pacotes para a porta de saída apropriada, e deve permitir que estações em segmentos separados transmitam simultaneamente, já que comuta pacotes utilizando caminhos dedicados.

Colisões não ocorrerão, porém poderá ser experimentada a contenção de dois ou mais quadros que necessitem do mesmo caminho ao mesmo tempo, que são transmitidos posteriormente graças aos buffers de entrada e saída das portas.

Alguns Switches, os de Workgroup, suportam somente uma estação ligada por porta, enquanto em outros, os de Backbone congestionado, segmentos com múltiplas estações são ligados a cada porta.

Em projetos da atualidade em rede, switches são utilizados não só para a interconexão, mas também para proporcionar um alargamento de banda disponível. Esses equipamentos têm um reservatório de banda, que são distribuídos por suas portas, visando se adequar às necessidades de desempenho específico do projeto em questão.

O Switch deve ser usado quando existem situações em que é desejada uma melhora de desempenho.

Repetidores

Lembra-se daquelas limitações sobre o comprimento do cabeamento? Conforme explicamos, os repetidores são um meio de contornar isso. Esses dispositivos repetem o sinal de transmissão, permitindo que sua rede se estenda muito mais do que normalmente poderia. Eles não são exatamente dispositivos de interconectividade, mas sim dispositivos para estender um pouco mais uma rede existente.

Bridge

Bridge é um produto com a capacidade de segmentar uma rede local em sub-redes, com o objetivo de reduzir tráfegos de mensagens na LAN (aumento de performance), ou converter diferentes padrões de LAN's (de Ethernet para Token Ring, por exemplo).

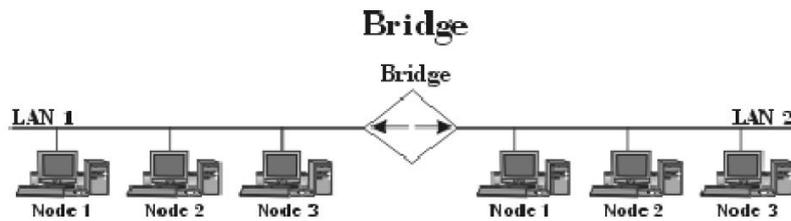
As Bridges manipulam pacotes, enquanto os repeaters manipulam sinais elétricos. As Bridges têm vantagens sobre os repeaters, porque não retransmitem ruídos, erros, ou frames de formação ruim (um frame deve estar completamente válido para ser transmitido por um Bridge).Conectam duas LAN's de mesmos protocolos. As Bridges atuam lendo o campo de endereço de destino dos pacotes de mensagens e transmitindo-os quando se tratar de segmentos de rede diferentes, utilizando o mesmo protocolo de comunicação.

Algumas das atribuições das Bridges são:

- Filtrar as mensagens de tal forma que somente as mensagens endereçadas a ela sejam tratadas.
- Armazenar mensagens quando o tráfego for muito grande.
- Funcionar como uma estação repetidora comum.

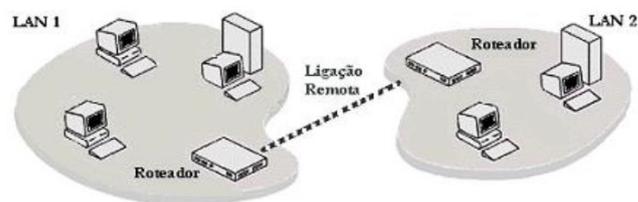
As Bridges também atuam como elementos passivos gerenciadores de rede, e pode coletar dados estatísticos de tráfego de pacotes para elaboração de relatórios.

São equipamentos usados para interligar duas LAN's localizadas a uma curta distância, ainda que ambas utilizem diferentes meios de transmissão. Protegem a rede resultante em

relação à passagem de perturbações elétricas e erros relativos a dados, mas não em relação a erros vindos dos níveis superiores do protocolo.

Roteadores

Roteador ou Router é um equipamento responsável pela interligação entre Redes LAN's atuando nas camadas 1, 2 e 3 do Modelo de Referência OSI (da ISO). Os Roteadores possuem como função, a decisão sobre qual caminho o tráfego de informações (Controle de dados) deve seguir, ou seja, decide por qual caminho deve seguir um dado pacote de dados recebido, isto é, a função do Roteador é fazer o encaminhamento dos pacotes entre duas redes através de regras, tais como:

- Rotas Estáticas inseridas no roteador.
- Rotas Dinâmicas nas quais o roteador consegue direcionar pacotes de dados recebidos por um determinado caminho.

Roteadores Internos

A performance se torna comprometida já que a CPU do PC atende às funções de roteamento e outras funções inerentes ao Sistema Operacional.

Roteadores Externos

Têm a combinação de placa de comunicação síncrona/assíncrona, PC, placa Ethernet e software de roteamento carregado ou bult-in no Sistema Operacional do PC (computador

pessoal). Trata-se de uma solução fácil, porém tem-se uma máquina não dedicada para o fim do roteamento, fazendo o papel do roteador.

O produto nesse caso é independente da arquitetura do hardware e software do servidor, porque a ligação ao servidor é feita via Ethernet e host do TCP/IP, ou algum outro protocolo de comunicação.

Os Roteadores interligam redes situadas a longas distâncias, e oferecem proteção relativa a erros associados aos níveis superiores do protocolo, como aqueles relacionados à falhas elétricas e relativas aos dados. Os Roteadores também são úteis para controlar a velocidade de transmissão dos pacotes, porque as redes possuem diferentes capacidades de transmissão e recepção, o que pode causar embaraço na rede.

São formados por HW (hardware) e SW (software) dedicados ao roteamento, e estando concentrados. Como têm funções exclusivamente voltadas ao roteamento, seu desempenho atinge índices superiores, e mostrando o porquê desses roteadores serem mais caros do que os outros.

Vantagens

- Eles podem ligar fisicamente redes rápidas, como a Ethernet local, a uma linha telefônica mais lenta.
- As Bridges permitem a passagem do tráfego ou ignoram a existência, e só conseguem tratar dados em pacotes homogêneos, os Roteadores são mais inteligentes e sofisticados. Os programas dos Roteadores lêem informações complexas de endereçamento e tomam decisões sobre como encaminhar os dados através dos diversos links que interligam as redes.

Desvantagens

- Os Roteadores são específicos de protocolo, ou seja, a maneira como um host fala com um roteador IP é diferente da maneira como fala com um roteador da Novell ou DECnet.
- Roteadores não podem ser utilizados para micro-segmentação onde os limites do número de modos compartilhados de um segmento aumentam a banda passante disponível. Em geral, os roteadores devem ser colocados no centro da rede.

Brouters

Os Brouters combinam as melhores características dos bridges e dos roteadores, eles podem trabalhar com protocolos de alto nível diferente e podem endereçar dados ao longo do caminho mais rápido na rede.

Naturalmente eles têm seus problemas, também, tais como, os brouters são muito caros e dão dor de cabeça para configurar, já que precisam ser ajustados minuciosamente para a rede em que vão trabalhar (todos os administradores de rede que usam brouters têm cabelos brancos). Em um complexo ambiente de múltiplas plataformas com centenas de nós, entretanto, os brouters oferecem melhor desempenho. Eles são um sofrimento real para configurar, mas uma vez que você tenha conseguido configurar, eles são excelentes.

Gateways

Os gateways atuam em todas as camadas do modelo OSI (da ISO), e têm como função fazer a interligação de redes distintas, isto é, seu objetivo é permitir a comunicação entre duas redes com arquiteturas diferentes (usando protocolos distintos, com características distintas).

Podem ser chamados de "roteadores de alta velocidade".

Os gateways redirecionam o tráfego de redes que utilizam diferentes meios e, algumas vezes, protocolos de comunicação diferentes. Eles resolvem problemas de diferença entre tamanho máximo de pacotes, forma de endereçamento, forma e controle de acesso, padrões de linguagem interna de formato de correios eletrônicos.

Um exemplo é que o gateway pode ser utilizado para interligar uma LAN Token Ring suportando arquitetura IBM/SNA, com uma LAN Ethernet (com arquitetura OSI), ou ainda com uma rede Apple Talk. É o equipamento mais caro e complexo para interconexão de redes, capaz de interpretar e traduzir os pacotes que processa. Geralmente é usado um sistema de processamento computacional completo para esta função, como por exemplo, estações de trabalho.

Outro exemplo de gateways (tirado do livro da Cyclades) pode-se citar um produto que integra redes TCP/IP com redes SNA.

Na figura abaixo qualquer nó da rede TCP/IP pode se conectar na rede SNA e ter acesso a um Mainframe, por exemplo, emulando terminais 3278.

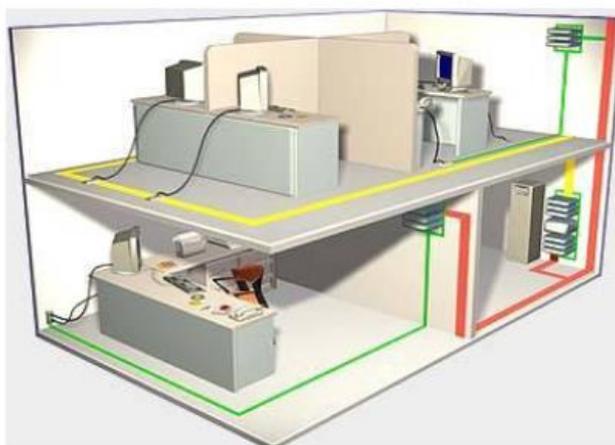
Exemplo de um gateway TCP/IP-SNA

Introdução ao cabeamento estruturado

A definição da rede estruturada baseia-se na disposição de uma rede de cabos, integrando os serviços de voz, dados e imagens que, facilmente pode ser redirecionada no sentido de prover um caminho de transmissão entre quaisquer pontos desta rede. Numa rede projetada seguindo este conceito, as necessidades de todos os usuários podem ser atendidas com facilidade e flexibilidade.

Cabeamento estruturado

É um cabeamento para uso integrado em comunicações de voz, dados e imagem, preparado de tal forma que atende aos mais variados layouts de instalação, por um longo período de tempo, sem exigir modificações físicas da infra-estrutura. Um só cabeamento atende diferentes tipos de redes de sinal em baixa tensão, como por exemplo, telefonia, redes locais de computação, sistema de alarme, transmissão de sinal de vídeo, sistemas de inteligência predial, automação predial e industrial.

O cabeamento estruturado originou-se de sistemas telefônicos comerciais, onde o usuário constantemente mudava sua posição física no interior de uma edificação. Desta forma, foi projetado o cabeamento de maneira a existir uma rede de cabos fixa horizontalmente, ligada a uma central de distribuição. Na central de distribuição, fazendo a escolha do cabo determinado, cada ponto da rede pode ser ativado ou desativado, alternando-se assim a posição da tomada por meio de uma troca de ligações. A evolução do sistema fez com que a central de distribuição pudesse se interligar a diversos tipos de redes, mantendo fixo, o cabeamento horizontal, e as tomadas são de múltiplo uso. Desta maneira acrescentaram-se as redes de computação, sistema de alarme, sinal para automação de processos, sinal de vídeo, etc.

Normas e sistemas

Atualmente o cabeamento estruturado baseia-se em normas internacionais, que direcionam os fabricantes para um certo conjunto de soluções próximas, evitando as constantes alterações de produtos, bem como, evitam sistemas “proprietários”, onde um só fabricante é detentor da tecnologia. A Norma Americana é EIA/TIA-568, “Commercial Building Telecommunications Wiring Standard”. A nível internacional temos a ISO/OSI (Open Systems Interconnection). Na Europa grande parte dos fabricantes utiliza o sistema IBCS (Integrated Building Cabling System). As variações que existem entre uma e outra, no entanto, deve-se mais às categorizações e conceitos, porém, assemelham-se tecnicamente. As iniciativas das normas vão, no sentido de uma arquitetura aberta, independente de protocolo. Desta forma, as novas tendências se desenvolvem já considerando este cabeamento, como é o caso do 100BaseT, do ATM e outros.

Projeto e infraestrutura

Este grande avanço dos sistemas de comunicação aprimorou e sofisticou bastante os projetos de edificações comerciais, industriais e residenciais. Hoje um edifício não pode, sob pena de nascer com altas deficiências, deixar de ter uma infraestrutura de cabeamento estruturado para redes de comunicação. Mesmo que de início não o utilize, pois as reformas e “emendas” são de alto custo, e nunca apresentam a qualidade necessária e desejável. A infra-estrutura de cabeamento estruturado é obrigatória em qualquer novo edifício, e deve interferir, em nível de projeto, desde o nascimento do projeto arquitetônico, pois o Cabeamento estruturado tem características próprias que vão interferir no projeto de um edifício de alta tecnologia.

Forma física de instalação

Justamente devido às altas freqüências em que o cabeamento deve operar, as condições físicas da instalação do cabeamento atingiram um alto grau de especialidade, que exige um projeto detalhado e com alto grau de planejamento. Em uma instalação com cabeamento estruturado não se utiliza, por exemplo, ligar diretamente um PC ao HUB. O que a norma prescreve é deixar preparado um cabeamento entre um patch panel e uma tomada. Na tomada pode-se ligar, ou não, um PC naquele ponto (ou um telefone, ou um sensor, um vídeo, etc), por sua vez ao painel distribuidor é conectado o equipamento ativo (HUB, central telefônica, CLP, head-end, etc). O sistema de cabeamento, portanto, deve ser aberto e independente, isto barateia e dá agilidade a todo o sistema, concentrando diversas redes em uma só.

Cabos

Para a instalação de um cabeamento estruturado para sinais de baixa tensão (voz, dados, imagens), utilizam-se cabos do tipo coaxial, cabos de par trançado e fibras óticas. Há uma tendência pelo uso prioritário dos cabos de par trançado e para a fibra ótica, devido à busca de melhor performance do cabeamento.

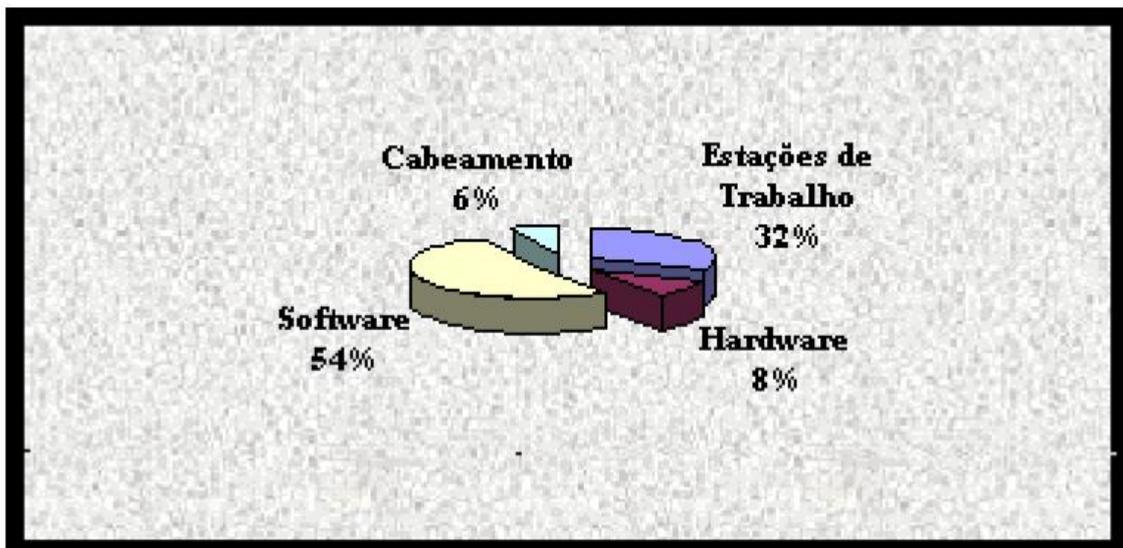
Para se obter um cabeamento de categoria 5 (até 100 MHz) conforme a EIA/TIA-568, teremos o uso de par trançado. A fibra ótica possibilita ainda melhores condições.

Certificações

Um cuidado especial deve ser tomado relativamente à certificação do cabeamento. Em que consiste tal certificação? As normas definem uma série de parâmetros para o cabeamento, tais como atenuação, comprimento real, mapeamento dos fios, paradiafonia, nível de ruído, que necessariamente devem estar dentro de uma faixa de valores pré-definidos.

A verificação destes valores é questão fundamental em um cabeamento, devendo ser feito com equipamentos especiais. É essa a garantia da instalação.

Estatísticas

Atualmente cerca de 70% dos problemas que acontecem em uma rede de computação, deve-se a problemas do cabeamento. “Os softwares costumam passar por uma evolução a cada 2 ou 3 anos, e de acordo com pesquisas, o hardware do seu PC geralmente tem uma vida útil de 5 anos. No entanto, você terá que viver 15 anos ou mais com seu cabeamento de rede” (Frank J. Derfler, Jr. e Les Freed). Outra estatística diz que em torno de 40% dos funcionários de uma empresa mudam de lugar uma vez por ano.E os custos para implantação completa de uma rede de computação estão aproximadamente divididos da seguinte forma:

Tendências

Todas as edificações sejam industriais, comerciais ou residenciais, devem desde já estar projetadas com a infra-estrutura de comunicações. Esta infra-estrutura influencia de tal modo os projetos, que um acompanhamento deve ser feito desde o início com o projeto de arquitetura e projeto elétrico, sensivelmente afetado por esta nova tecnologia.

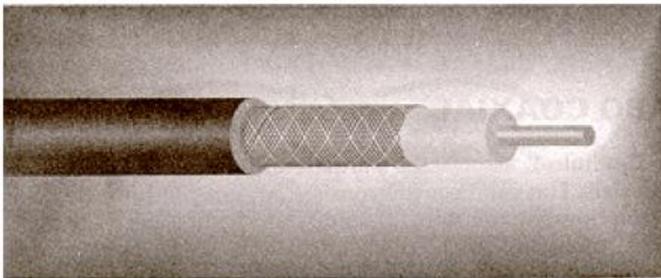
Cabeamento não estruturado

Em muitos ambientes de escritórios atuais, o cabeamento da rede de dados foi instalado de forma incremental, respondendo a modificações na tecnologia, necessidades de rede e planos da companhia. Tipicamente, isso deixa um legado de sistemas incompatíveis que podem incluir sistemas de chaveamento telefônico, mainframe ou sistemas de minicomputador. Uma vez que cada sistema está instalado de acordo com seu próprio critério de cabeamento, usando tipos diferentes de cabos, eles são de difícil interconexão e especialmente difíceis de manter e expandir. Essa situação é típica do sistema de cabeamento não estruturado, onde não há um conjunto de padrões para interconexão. Embora os custos iniciais sejam comparativamente baixos para o cabeamento não estruturado, as dificuldades a longo prazo e custos de integração ou substituição de sistemas de cabeamento incompatíveis são consideráveis.

Cabeamento proprietário

Os fornecedores maiores estiveram entre os primeiros a perceber a importância do cabeamento estruturado, respondendo com plantas de cabeamento pré-planejadas, que garante o funcionamento correto de seus dispositivos numa rede. Companhias telefônicas foram alguns dos líderes, baseadas em sua experiência com a instalação de cabo telefônico.

Tipos de cabos

Cabo coaxial

O termo "coaxial" surgiu porque o condutor central e a malha de blindagem têm o mesmo eixo.

O cabo coaxial, freqüentemente conhecido como cabo BNC (Bayonet Naur - um conector em forma de baioneta para cabos coaxiais finos), é feito de um único fio de cobre revestido por isolante e coberto por uma camada de trança de alumínio ou de cobre que protege o fio da interferência externa. Se você precisar de mais largura de banda e proteção contra ruídos do que o par trançado, mas não pode gastar com fibra ótica, o coaxial é o caminho, porém, é muito mais lento.

Par trançado

Conector RJ-45

É um cabo composto por dois ou quatro pares de fios envolvidos por uma camada isolante. Os dois fios são enrolados em espiral, a fim de reduzir o ruído (interferência) e manter as propriedades elétricas do meio constantes por todo o seu comprimento. Cada par é trançado com um número variado de tranças por metro.

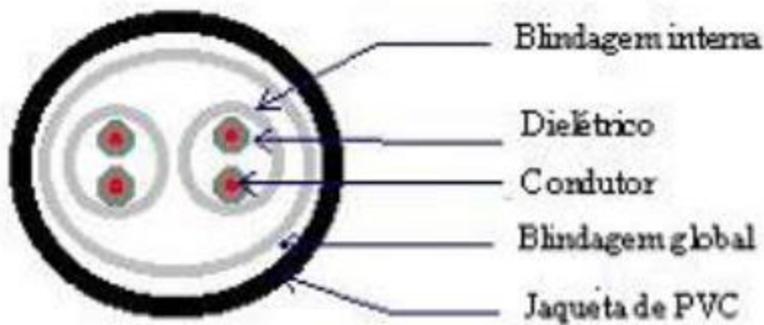
Utiliza-se um conector RJ-45.Todo meio de transmissão sofre influência do meio externo, o que prejudica o desempenho na taxa de transmissão. Essas perdas podem ser atenuadas diminuindo a distância entre os pontos a serem ligados.

Para se contornar os problemas da interferência e do ruído, foram criados os cabos de “par trançado com blindagem”.

Sua transmissão pode ser tanto analógica quanto digital. Para se saber qual a sua taxa máxima de transmissão e a distância máxima permitida, é necessário levar em conta a perda de energia, que pode ocorrer por radiação ou por calor (dissipação). A perda de energia aumenta com a distância, até chegar um ponto onde o receptor não consegue mais reconhecer o sinal. Em geral, um par trançado pode chegar até algumas dezenas de metros com taxas de transmissão da ordem de alguns megabits por segundo. A taxa de transmissão pode variar entre 9600 a 19200 bps. É o cabo mais utilizado, mesmo tendo sua força a longas distâncias inferiores ao cabo coaxial.

Os cabos de par trançado são classificados em dois grupos, de acordo com a blindagem do condutor:

Par trançado com blindagem - (STP - Shielded Twisted Pair)

Blindagem interna
Dielétrico
Condutor
Blindagem global
Jaqueta de PVC

Possui uma blindagem interna, ou seja, cada par ou grupo de fios é envolvido por uma malha ou trança metálica, que funciona como uma barreira para os sinais de interferência, porém ocupa mais espaço físico, portanto, um maior volume de blindagem e isolamento aumenta o tamanho, o peso e o custo. A blindagem é aterrada nas duas extremidades, portanto, a blindagem não faz parte do caminho percorrido pelo sinal. Também usa conector RJ-45.

Possui alta taxa de sinalização, com poucas chances de distorção do sinal.

Blindado de 100 ohms

Este é o STP mais simples, pois, contém uma blindagem formada por uma folha de cobre ao redor de todos os seus fios.

Blindado de 150 ohms

Este é o STP mais comum, com impedância de 150 ohms, que suporta 300 MHz de largura no máximo em 100m de cabo. Além de todo o cabo ser blindado para reduzir a interferência eletromagnética e de radiofreqüência, há uma blindagem que separa cada par de fios trançados, para diminuir a diafonia (ruídos elétrico produzidos por sinais de outros fios do cabo).

O STP de 150 ohms é normalmente utilizado em redes Token Ring da IBM, enquanto que os de 100 ohms são mais utilizados em instalações Ethernet.

Par trançado sem blindagem - (UTP - Unshielded Twisted Pair)

Padronizado pelo IEEE 802.3, também conhecido como 10BaseT. Esse cabo é composto por quatro pares de fios, sendo cada par isolado um do outro e todos são trançados juntos dentro de uma cobertura externa.Não havendo blindagem física interna, sua proteção é encontrada através do "efeito de cancelamento" dos pares de fios trançados, onde mutuamente reduz a interferência eletromagnética de radiofreqüência e a diafonia.

No cancelamento, o fluxo de corrente de um fio cria um pequeno campo magnético circular ao redor dele. A direção do fluxo de corrente do fio determina a direção das linhas de força eletromagnética que o circundam. Se dois fios estiverem no mesmo circuito elétrico, os elétrons fluirão da fonte de voltagem negativa para a carga (destino) de um fio, e daí para a fonte positiva de outro fio. Se os dois fios estiverem próximos, seus campos eletromagnéticos serão o oposto um do outro. Isso fará com que eles se cancelem e anulem também campos externos.

os cabos UTP são divididos em 5 categorias. Para isso, são levados em conta os níveis de segurança e a bitola dos fios (números maiores indicam fios com diâmetros menores).

Categorias

Cada tipo de cabo, conforme o especificado acima, vem atender determinadas necessidades e tipos de soluções diferentes, sendo assim, opções de solução em uma instalação.

- Categoria 1

Este cabo nada mais é que o antigo fio telefônico usado na maior parte das residências, e usado em sistemas telefônicos comerciais até 1983 no Estados Unidos. Ele não é conveniente para a transmissão de dados de alta velocidade, uma vez que seu único requisito é ser trançado.

- Categoria 2

Este tipo de cabo é certificado para transmissão de dados até 4 Mbps, UTP tipo 3 definido pela IBM, tem baixa taxa de transmissão, ou seja, quatro pares trançados não-blindados e sólidos de fios para transmissão de voz e dados.

- Categoria 3

Este é o cabo de mais baixa classificação que você pode usar com qualquer rede local. Ele pode transmitir até 10 Mbps e é mais bem construído que o cabo das categorias 1 e 2.

- Categoria 4

Para redes Token Ring de 16 Mbps, este é o cabo de grau mais baixo que você pode usar. De fato, para conseguir o melhor uso de sua rede local, você deve considerar esta categoria como sendo o padrão mínimo, em lugar do cabo de categoria 3.

- Categoria 5

Para transmissões em velocidades reais, este é o par trançado que você quer. Ele oferece baixo nível de interferência e velocidade máxima em transmissão de ofuscantes 100 Mbps.

O cabo categoria 5 é o cabo indicado na especificação Fiber Distributed Data Interface (FDDI), que definiu a coexistência de fio de cobre e fibra óptica no mesmo ambiente. Ele é projetado para funcionar em conjunto com o cabo de fibra ótica para fornecer throughput (medida de velocidade de transferência de dados) melhorado para soluções multimídia (áudio e vídeo) em rede.

- Categoria 5e

Cabos com capacidade de transmissão, ainda, de até 100 Mbps (com melhora na resposta do cabo para as freqüências maiores).

- Categoria 6

Cabo com capacidade de transmissão mínima de 100 Mbps, substitui o cabo categoria 5e, pois possui uma melhor comunicação com o cabo de Fibra Óptica.

Configuração das pontas

Padrão 568A

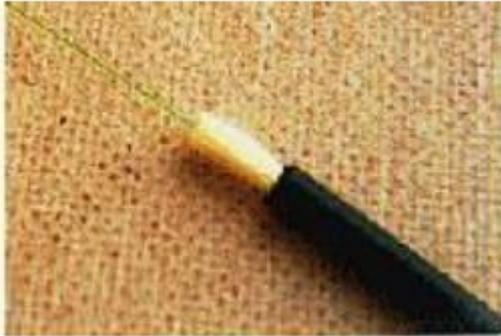
1 Branco do verde
2 Verde
3 Branco do Laranja
4 Azul
5 Branco do Azul
6 Laranja
7 Branco do Marrom
8 Marrom

Padrão 568B

1 Branco do Laranja
2 Laranja
3 Branco do verde
4 Azul
5 Branco do Azul
6 Verde
7 Branco do Marrom
8 Marrom

Cabo Paralelo: Configuração padrão, o cabo possui duas pontas iguais

Cabo Crossover: Para uma rede ponto a ponto com apenas duas máquinas use um padrão para cada ponta.

Fibra óptica

É constituído de um filamento denominado núcleo, por onde é feita a transmissão da luz. Em geral, o material dielétrico (filamento), é constituído de sílica ou plástico, em forma cilíndrica transparente e flexível, de dimensões microscópicas comparáveis às de um fio de cabelo

Esta forma cilíndrica é envolvida por uma camada de material também dielétrico, chamada casca.

Ao redor do filamento existem substâncias de menor índice de refração, que fazem com que os raios de luz sejam refletidos internamente.

O índice de refração é a grandeza que expressa a velocidade da luz num meio de transmissão. É definido como sendo n= cv, onde c é a velocidade da luz no vácuo e a velocidade da luz no meio em questão. O índice de refração depende do comprimento de onda da luz, o que vai provocar a dispersão do impulso luminoso na fibra ótica, limitando a capacidade de transmissão dos sinais.

A fibra transmite os dados via pulsos de luz codificados, dentro do domínio do infravermelho (10xE14 a 10xE15 Hz), que podem ser gerados por um LED ou laser. Necessitam de um conversor de sinais elétricos para sinais óticos, um transmissor, um receptor e um conversor de sinais óticos para sinais elétricos. Existem duas fibras por cabo.

Transmissores ópticos

São responsáveis pela conversão de sinais elétricos em sinais óticos, que serão transmitidos pela fibra. A fonte ótica é modulada pela sua intensidade, através da variação da corrente elétrica injetada no gerador ótico. A fonte ótica é um semicondutor e pode ser LED ou LASER, quando LED (Light Emitting Diode) utiliza o processo de fotogeração por recombinação espontânea.

São utilizados em sistemas de comunicação que possuem taxas de transferência menor que 200 Mbps e quando Diodo LASER (Light Amplification by Simulated Emission on Radiation): utiliza o processo de geração estimulada de luz.

O Laser é melhor que o LED, como mostra a tabela abaixo:

Característica	Laser	Led
Potência ótica	alta	baixa
Custo	alto	baixo
Utilização	complexa	simples
Tempo de vida	menor	maior

Receptores ópticos

Também conhecidos como fotodetectores, convertem sinais óticos recebidos pela fibra em sinais elétricos.

Os fotodetectores mais usados são os fotodiodos e os mais comuns são PIN e APD (Avalanche PhotoDiode).

Características	PIN	ADP
Sensibilidade	menor	maior
Relação Sinal/ruído	pior	melhor
Custo	baixo	alto
Vida útil	maior	menor
Tempo de resposta	maior	menor

Fibras multímodo de índice gradual

Ao invés de uma mudança abrupta do índice de refração do núcleo para a casca, esse índice diminui gradualmente de forma contínua.

Utiliza emissores do tipo LED, que diminui seu custo e a taxa média de transmissão dessa fibra gira em torno de 100 Mbps. Necessita de um repetidor a cada 2 Km.

Fibras multímodo degrau

São as mais simples. O funcionamento dessas fibras é baseado no fenômeno de reflexão total interna na casca de índice de refração menor. O termo degrau vem da existência de uma descontinuidade na mudança de índice de refração na fronteira entre o núcleo e a casca da fibra.

É denominado multímodo, pois é possível que vários feixes em diferentes ângulos de incidência se propaguem através de diferentes caminhos pela fibra e a taxa de transmissão varia entre 15 e 25 MHz/Km.

Fibras monomodo

A luz percorre a fibra em um único modo e em linha reta.

Esse tipo de fibra é insensível à dispersão modal, que é a reflexão da onda luminosa em diferentes tempos. O diâmetro do núcleo é muito pequeno.

Utiliza o laser como emissor dos sinais de luz, o que lhe permite longas distâncias (até 50 Km), sem a necessidade de um repetidor e pode atingir taxas de transmissão da ordem de 1 Gbps.

Para todos os tipos, a atenuação das transmissões não depende da freqüência utilizada, o que torna a taxa de transmissão muito mais alta, em torno de ~100.000 Mbps, podendo chegar a 200.000 Mbps e a 620 Mbps numa única fibra unidirecional.

É totalmente imune a interferências eletromagnéticas e a ruídos, não precisa de aterramento e mantém os pontos que liga eletricamente isolados um do outro. Porém, a atenuação pode ser causada pela absorção feita pelo meio físico de transmissão ou pela dispersão modal.

Podem chegar à distância de 50 Km, sem a necessidade de um repetidor.

Suporta voz, dados, vídeo e são mais finas e mais leves que os cabos coaxiais, o que facilita sua instalação. Porém, por ser inflexível, requer cuidados especiais na instalação e manutenção.

Por incrível que possa parecer, ainda existem algumas limitações quanto à fibra ótica:

- A junção das fibras é uma tarefa muito delicada e cara, pois as dimensões da fibra são muito pequenas e requerem alta precisão. Não pode haver dobra nos cabos de fibra ótica, pois pode tornar o ângulo de incidência dos feixes de luz em relação à normal muito pequeno, provocando o escape desses feixes da fibra, pois não chegarão a sofrer reflexão. São muito frágeis, quebrando com facilidade.
- Os componentes óticos não possuem uma padronização.

Apesar das limitações acima, possui inúmeras vantagens:

- Permite enviar mais dados por longas distâncias e pequeno tamanho e peso;
- São imunes a interferência eletromagnética, radiofreqüência e diafonia;
- É constituído de material isolante, o que lhe concede isolação elétrica;
- Alta confiabilidade no sinal transmitido, pois não irradiam significativamente a luz transportada e matéria prima abundante.

Wireless - Redes sem fio

A tecnologia Wireless (sem fio) permite a conexão entre diferentes pontos sem a necessidade do uso de cabos (nem de telefonia, nem de TV a cabo, nem de fibra óptica), através da instalação de uma antena e de um rádio de transmissão.

Desta forma, pode-se navegar pela Internet desde o escritório, um bar, um aeroporto, um parque, etc

IEEE - Instituto de Engenheiros Eletricistas e Eletrônicos

O Instituto de Engenheiros Elétricos e Eletrônicos ou IEEE é a maior, em número de sócios, organização profissional do mundo. O IEEE foi formado em 1963 pela fusão do Instituto de Engenheiros de Radio (IRE) com o instituto Americano de Engenheiros Eletricistas (AIEE).

O IEEE tem filiais em muitas partes do mundo, sendo seus sócios engenheiros elétricos, engenheiros da computação, cientistas da computação, profissionais de telecomunicações etc. Sua meta é promover conhecimento no campo da engenharia elétrica, eletrônica e da computação Um de seus papéis mais importantes é o estabelecimento de padrões para formatos de computadores e dispositivos.

IEEE 802.11

É o padrão especifico do IEEE que cuida das redes sem fio. Que também são conhecidas como redes Wi-Fi ou Wireless.

Wi-Fi

Foi uma marca licenciada originalmente pela Wi-Fi Alliance para descrever a tecnologia de redes sem fio embarcadas (WLAN) baseadas no padrão IEEE 802.11.

O padrão Wi-Fi opera em faixas de freqüências que não necessitam de licença para instalação e/ou operação. Este fato as torna atrativas. No entanto, para uso comercial no Brasil é necessária licença da Agência Nacional de Telecomunicações (Anatel). Para se ter acesso à internet através de rede Wi-Fi deve-se estar no raio de ação de um ponto de acesso (normalmente conhecido por (hotspot) ou local público onde opere rede sem fios e usar dispositivo móvel, como laptop.

Como funcionam?

Através da utilização de portadoras de rádio ou infravermelho, as redes wireless estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Num ambiente típico, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também vão intermediar o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roaming semelhante a um sistema de telefonia celular.

Classificação das redes sem fios

WPAN

Wireless Personal Area Network ou rede pessoal sem fio. Normalmente utilizada para interligar dispositivos eletrônicos fisicamente próximos. Nos equipamentos mais recentes é utilizado o padrão Bluetooth para estabelecer esta comunicação, mas também é empregado raio infravermelho (semelhante ao utilizado nos controles remotos de televisores).

WLAN

Wireless Local Area Network. WLAN já é muito importante como opção de conexão em muitas áreas de negócio. Inicialmente os WLANs assim distante do público em geral foi instalado nas universidades, nos aeroportos, e em outros lugares públicos principais.

WMAN (Wi-Max)

Trata-se de uma tecnologia de banda larga sem-fio, capaz de atuar como alternativa a tecnologias como cabo e DSL na construção de redes comunitárias e provimento de acesso de última milha. Em teoria, espera-se que os equipamentos Wi-Max tenham alcance de até 50 Km e capacidade de banda passante de até 70 Mbps. Na prática, alcance e banda dependerão do equipamento e da freqüência usados, e se a antena de um ponto consegue "ver" a antena de outro, se não há obstáculos no caminho – construções, montanhas.

WWAN

Wireless Wide Area Network. É a rede geograficamente infinita via comunicação sem fio, hoje encontramos diversas empresas que comercializam a internet sem fio.

Principais padrões

802.11A

Chega a alcançar velocidades de 54 Mbps dentro dos padrões da IEEE e de 72 a 108 Mbps por fabricantes não padronizados. Esta rede opera na freqüência de 5 GHz e inicialmente suporta 64 utilizadores por Ponto de Acesso (PA). As suas principais vantagens são a velocidade, a gratuidade da freqüência que é usada e a ausência de interferências. A maior desvantagem é a incompatibilidade com os padrões no que diz respeito a Access Points 802.11 b e g, quanto a clientes, o padrão 802.11a é compatível tanto com 802.11b e 802.11g na maioria dos casos, já se tornando padrão na fabricação dos equipamentos.

802.11b

Alcança uma velocidade de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes não padronizados. Opera na freqüência de 2.4 GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis, fornos microondas e dispositivos Bluetooth. O aspecto positivo é o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo mundo. O 802.11b é amplamente utilizado por provedores de internet sem fio.

802.11g

Baseia-se na compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 54 Mbps. Funciona dentro da frequência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens

também são as velocidades). Usa autenticação WEP estática. Torna-se por vezes difícil de configurar, como Home Gateway devido à sua freqüência de rádio e outros sinais.

802.11n

Tem uma largura de banda até aos 300 Mbps e um alcance de 70 metros. Opera nas frequências 2,4GHz e 5GHz. É um padrão recente com uma nova tecnologia, MIMO (multiple input, multiple output) que utiliza várias antenas para transferência de dados de um local para outro. Os principais benefícios desta tecnologia são o aumento significativo da largura de banda e o alcance que permite.

Outros padrões:

- 802.11d
- 802.11e (agrega qualidade de serviço (QoS)
- 802.11f
- 802.11h
- 802.11i
- 802.11j
- 802.11k
- 802.11m
- 802.11p
- 802.11r
- 802.11s
- 802.11t
- 802.11u
- 802.11v

Tecnologias

IrDA

Infrared Data Association, comunicação infra-vermelho, para pequenas distancias

Bluetooth

Bluetooth é uma tecnologia para a comunicação sem fio entre dispositivos eletrônicos a curtas distâncias.

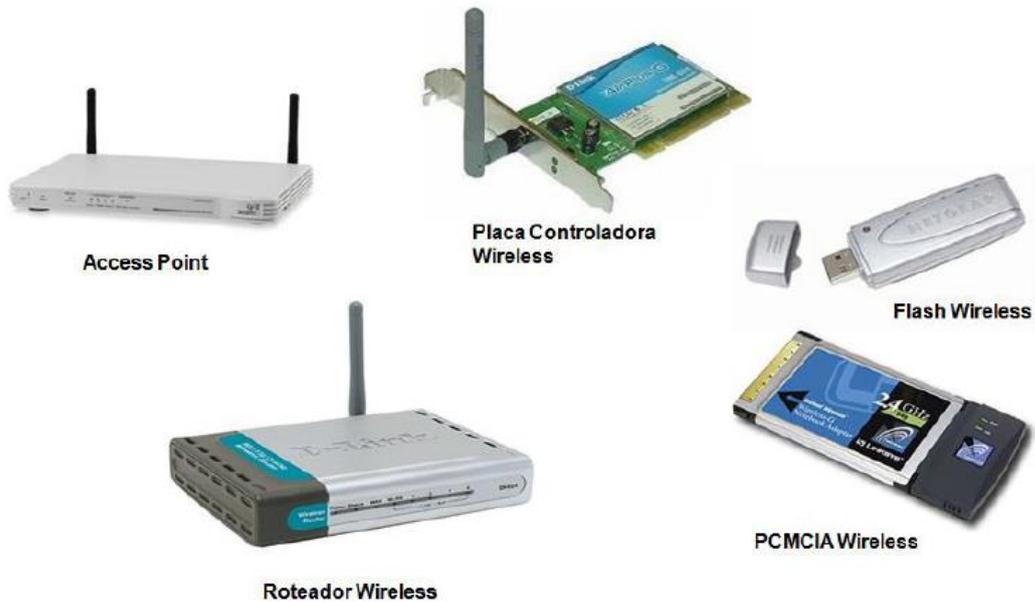
Equipamentos Wireless

Access Point

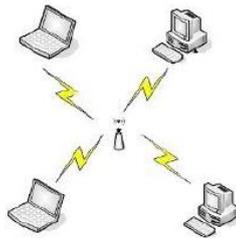
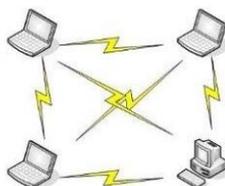
Placa Controladora Wireless

Flash Wireless

Roteador Wireless

PCMCIA Wireless

Modos de operação

Em termos organizacionais, o padrão 802.11 define dois modos distintos de operação: Ad-Hoc e infra-estrutura.

No modo infra-estrutura é usado o Access Point para concentrar todo tráfego da rede.

No modo Ad-Hoc não existe um concentrador, ou seja, os equipamentos se conectam diretamente uns aos outros.

Estendendo alcance, layout avançado de rede

Às vezes o plano de rede básica não funciona devido ao alcance, obstáculos como paredes e lajes, ou o layout geral do ambiente. Quando isto acontecer existem algumas opções e todas elas têm várias vantagens e desvantagens.

Se o alcance só precisa estender por 50 ou 70 metros, um ou mais Access Points Repetidores podem ser ligados à rede. Estes pequenos equipamentos funcionam como um Access Point trabalhando num modo especial que permite a integração de dois ou mais Access Points em uma única rede. Para configurar o repetidor, você deve plugá-lo à sua rede física através de um cabo Ethernet Categoria 5E e configurá-lo. Após essa configuração você poderá movê-lo para seu local definitivo. Os repetidores podem normalmente dobrar o alcance efetivo da rede Wireless, permitindo que mais computadores sejam ligados à rede. Os repetidores podem ser adicionados conforme a necessidade para estender a rede com algumas limitações.

Layout

As dimensões físicas da área e o número de computadores que precisam de acesso de rede determinam o tipo de equipamento de Rede sem fios necessário. Se todos os computadores estão em uma área pequena, digamos um escritório não mais do que 50 metros, com algumas paredes, tudo de que se precisa são: (1) adaptador de rede de Rede sem fios por computador e (1) Access Point Wireless (ou Roteador se uma conexão de banda larga precisa ser compartilhada).

Para configurar a rede, instale um adaptador de rede de Rede sem fios em cada computador e ligue o Access Point ou Roteador em uma posição central.

Otimizando o sinal

O alcance típico de uma rede 802.11g é de 30 metros em espaços fechados (como uma casa ou um prédio, onde existem paredes e outros obstáculos) e 150 metros em campo aberto, sem obstáculos.

Se você possui um roteador wireless comprado a preços baixos, saiba que sua antena é de 2dbi, ou seja, o alcance é mínimo para áreas com muitas paredes e, com certeza, você vai ter muita dor de cabeça caso sua vontade for de aumentar o sinal. Nesses casos, o ideal seria usar uma antena de 5dbi, cujo alcance é bem maior e mais limpo, sem oscilações.

Para alcançar o melhor sinal com a menor interferência da mobília e dispositivos elétricos mantenha o Ponto de Acesso a cerca de 1,60m de altura. Coloque o Access Point em uma estante, armário, ou monte-o na parede.

Advertência: Nunca instale um Access Point dentro de um espaço fechado. Isso causa muita degradação de sinal e poderá causar aquecimento do AP. Mantenha-o em uma área aberta, se possível.

Segurança

Na criptografia se faz o uso de uma chave (KEY) para codificar os dados que são transferidos. A chave é determinada pelo tamanho, por exemplo 64bits, 128bits, 256bits. Quanto maior a combinação de bits, mais forte fica a criptografia, e consequentemente a segurança.

Protocolos de segurança

WEP

Significa Wired Equivalent Privacy.

O WEP se encarrega de "encriptar" os dados transmitidos através da rede.

Existem dois padrões WEP, de 64 e de 128 bits. O primeiro é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede.

É muito inseguro devido a sua arquitetura.

WPA

Significa Wi-Fi Protected Access

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves

por pacotes, além de possuir função detectora de erros, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação se utiliza do 802.11x e do EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede.

WPA2

É o Avanço do WPA

O WPA2 é a modalidade de segurança sem fio mais forte.

Introdução ao TCP/IP

O desenvolvimento da arquitetura Internet, Transmission Control Protocol/Internet Protocol (TCP/IP) foi patrocinado pela Defense Advanced Research Projects Agency (DARPA). O TCP/IP é um conjunto de protocolos desenvolvidos para permitir que computadores compartilhem recursos dentro de uma rede. Em uma definição mais básica, o nome correto para este conjunto de protocolos é "Conjunto de Protocolos Internet". Os protocolos TCP e IP são dois dos protocolos deste conjunto. Como os protocolos TCP e IP são os mais conhecidos, é comum se referir a TCP/IP para referenciar toda a família de protocolos.

Na família de protocolos TCP/IP, alguns protocolos, como TCP, IP e User Datagram Protocol (UDP), provêm funções de baixo nível, necessárias a diversas aplicações. Os outros protocolos são execução de tarefas específicas, como por exemplo, transferência de arquivos entre computadores, envio de mensagens. Os serviços TCP/IP mais importantes são:

Transferência de Arquivos - o File Transfer Protocol (FTP), permite a um usuário em um computador copiar arquivos de outro computador, ou enviar arquivos para um outro computador. A segurança é garantida requerendo-se que o usuário especifique um username e uma senha, para acesso ao outro computador.

Login Remoto - o Network Terminal Protocol (TELNET), permite que um usuário se log (tenha uma sessão de trabalho) em um outro computador da rede. A sessão remota é iniciada especificando-se o computador em que se deseja conectar. Até que a sessão seja finalizada, tudo o que for digitado será enviado para o outro computador. O programa de TELNET faz com que o computador requisitante seja totalmente invisível, tudo é enviado diretamente ao computador remoto.

Eletronic Mail (SMTP) - permite ao usuário enviar mensagens para usuários em outro computador. Deve ser mantido um arquivo de mail para cada usuário, e o sistema de mail simplesmente adicionará novas mensagens a este arquivo de mail. Quando um usuário vai enviar um mail, o programa espera ser capaz de manter uma conexão com o computador destino, para que a mensagem possa ser enviada.

O protocolo TCP/IP é baseado em um modelo que pressupõe a existência de um grande número de redes independentes conectadas através de gateways. Um usuário pode ter acesso a computadores ou outros recursos em qualquer uma destas redes. As mensagens, muitas vezes, passam por uma grande quantidade de redes para atingirem seus destinos. O roteamento destas mensagens deve ser completamente invisível para o usuário. Assim para ter acesso a um recurso em outro computador o usuário deve conhecer o endereço Internet deste computador. Atualmente este endereço é um número de 32 bits, escrito como 4 números decimais, cada um representando 8 bits de endereço.

Internet Protocol (IP)

O protocolo IP, padrão para redes Internet, é baseado em um serviço sem conexão. Sua função é transferir blocos de dados, denominados datagramas, da origem para o destino, onde a origem e o destino são hosts identificados por endereços IP. Este protocolo também

fornece serviço de fragmentação e remontagem de datagramas longos, para que estes possam ser transportados em redes onde o tamanho máximo permitido para os pacotes é pequeno.

Como o serviço fornecido pelo protocolo IP é sem conexão, cada datagrama é tratado como uma unidade independente que não possui nenhuma relação com qualquer outro datagrama. A comunicação é não-confiável, pois não são utilizados reconhecimentos fim-a-fim ou entre nós intermediários. Não são empregados mecanismos de controle de fluxo e de controle de erros. Apenas uma conferência simples do cabeçalho é realizada, para garantir que as informações nele contidas, usadas pelos gateways para encaminhar datagramas, estão corretas.

Atualmente utilizamos o IPV4, porém o IPV6 já será adotado como padrão nos próximos anos.

Transmission Control Protocol (TCP)

O TCP é um protocolo da camada de transporte da arquitetura Internet TCP/IP. O protocolo é orientado a conexão e fornece um serviço confiável de transferência de arquivos fim-a-fim. Ele é responsável por inserir as mensagens das aplicações dentro do datagrama de transporte, reenviar datagramas perdidos e ordenar a chegada de datagramas enviados por outro micro. O TCP foi projetado para funcionar com base em um serviço de rede sem conexão e sem confirmação, fornecido pelo protocolo IP.

O protocolo TCP interage de um lado com processos das aplicações e do outro com o protocolo da camada de rede da arquitetura Internet. A interface entre o protocolo e a camada superior consiste em um conjunto de chamadas. Existem chamadas, por exemplo, para abrir e fechar conexões e para enviar e receber dados em conexões previamente estabelecidas. Já a interface entre o TCP e a camada inferior define um mecanismo através do qual as duas camadas trocam informações assincronamente.

Este protocolo é capaz de transferir uma cadeia (stream) contínua de octetos, nas duas direções, entre seus usuários. Normalmente o próprio protocolo decide o momento de parar de agrupar os octetos e de, conseqüentemente, transmitir o segmento formado por esse agrupamento. Porém, caso seja necessário, o usuário do TCP pode requerer a transmissão imediata dos octetos que estão no buffer de transmissão, através da função push.

Conforme mencionado, o protocolo TCP não exige um serviço de rede confiável para operar, logo, responsabiliza-se pela recuperação de dados corrompidos, perdidos, duplicados ou entregues fora de ordem pelo protocolo de rede. Isto é feito associando-se cada octeto a um número de seqüência. O número de seqüência do primeiro octeto dos dados contidos em um segmento é transmitido junto com o segmento e é denominado número de seqüência do segmento. Os segmentos carregam “de carona” (piggybacking) um reconhecimento.

O reconhecimento constitui-se do número de seqüência do próximo octeto que a entidade TCP transmissora espera receber do TCP receptor na direção oposta da conexão. Por exemplo, se o número de seqüência X for transmitido no campo Acknowledge (ACK), ele indica que a estação TCP transmissora recebeu corretamente os octetos com número de seqüência menores que X, e que ele espera receber o octeto X na próxima mensagem.

Principais protocolos que formam o protocolo TCP/IP:

- ARP (Address Resolution Protocol) – Protocolo que por meio do numero IP localiza o numero MAC de um computador;
- RARP (Reverse Address Resolution) - Localiza o número MAC por meio do número de IP de um computador;
- ICMP (Internet Control Message Protocol) - Responsável pela geração das mensagens de erro e pacotes de teste. É uma extensão do protocolo IP;
- IGMP (Internet Group Management Protocol) – É um protocolo que gerencia as listas de partição da difusão seletiva IP em uma rede TCP/IP. A difusão seletiva IP é o processo no qual uma mensagem é transmitida para um grupo selecionado de destinatários;
- UDP (User Datagram Protocol) - Como o TCP, é responsável pela entrega dos dados, porém não garante a sua entrega;
- RIP (Routing Information Protocol) - Também é responsável pelo roteamento dos pacotes na rede;
- HTTP (Hypertext Transfer Protocol) - Protocolo que permite a transferência de documentos hipertexto. Por meio desse protocolo podemos receber as páginas da Internet;
- NNTP (Network News Transfer Protocol) - Esse protocolo é responsável pela transferência de mensagens de grupos do tipo news;
- SMTP (Simple Mail Transfer Protocol) - Protocolo responsável pelo envio e recebimento de e-mail;
- SNMP (Simple Network Management Protocol) - Estatísticas sobre o tráfego da rede podem ser executadas por intermédio desse protocolo;
- FTP (File Transfer Protocol) – Executa a transferência de arquivos entre sistemas. O FTP exige senha para entrada e pode "navegar" entre diretórios.
- IRC (Internet Relay Chat) - Esse protocolo implementa o serviço de chat;
- NFS (Network File System) - Esse protocolo é responsável pelo compartilhamento de arquivos remotos. Foi desenvolvido pela Sun;
- Telnet - Protocolo de emulação de terminal.
- DNS (Domain Name Server) - Tem por função auxiliar: na transparência da identificação de endereços IPs, inclusive endereços na Internet, para os usuários locais de um sistema computacional; manter uma tabela com os endereços dos caminhos de algumas redes na Internet que auxilie aos roteadores. A Figura Abaixo exemplifica uma parte de uma árvore de domínio da Internet. Desta figura podemos entender a importância do protocolo DNS no auxílio da procura de um endereço na rede. O UDP serve ao DNS de máquina local quando é necessária uma consulta a uma tabela DNS de um computador remoto.

Endereçamento IP

O Endereço IPV4 é um número de 4 bytes (ou 32 bits), separados por três pontos. Tem a função de informar o número da rede e o número dos computadores.

Os primeiros 8 bits (1º octeto) do número são responsáveis por determinar em que classe o endereço IP está.

Classe	1º octeto	2º octeto	3º octeto	4º octeto
A	*1 – 126*	*0 – 255*	*0 - 255*	*1 – 254*
	Rede	*Host*	*Host*	*Host*
B	*128 – 191*	*0 – 255*	*0 – 255*	*1 – 254*
	Rede	*Rede*	*Host*	*Host*
C	*192 – 223*	*0 – 255*	*0 – 255*	*1 – 254*
	Rede	*Rede*	*Rede*	*Host*

O endereçamento IPv4 é composto por dois níveis macros, NetId e HostId. O primeiro nível é composto pelo endereço de rede (NetId), que é fornecido pela IANA (Internet Assigned Number Authority), órgão gestor da Internet para atribuição de endereços. Por outro lado, o segundo nível (HostId) é de responsabilidade da organização. Desta forma, a atribuição dos endereços fica por conta da autoridade local da corporação.

O endereço da classe A foi imaginado para um ambiente no qual teríamos poucas redes e uma grande quantidade de computadores. Nesta classe de endereço, dispomos só o primeiro octeto (NetId). Os endereços de rede 0 (00000000) e 127 (01111111) são reservados, o que resulta no limite de 126 como endereços válidos. Quanto aos endereços de computadores na rede, temos 24 bits de endereços possíveis (28x 28x 28 = HostId x HostId x HostId).

O endereço da classe B foi projetado para um ambiente no qual teríamos uma quantidade equivalente no número de redes e de computadores. A classe B dispõe os dois primeiros octetos (NetId . NetId). Assim, nesta classe existem 214 endereços de rede. O limite dos endereços do primeiro octeto desta classe fica situado entre 128 (10000000) e 191 (10111111). Quanto aos endereços de computadores na rede, temos 16 bits de endereços possíveis (28x 28 = HostId x HostId).

O endereço da classe C é caracterizado por ser um ambiente imaginado para ter muitas redes e poucos computadores. Na classe C, os três primeiros octetos (NetId . NetId . NetId). Desta forma, nesta classe existem 221 endereços de rede. O limite dos endereços do primeiro octeto da classe C fica situado entre 192 (11000000) e 223 (11011111). Quanto aos endereços de computadores na rede, temos 8 bits de endereços possíveis (28 = HostId).

Outras Classes:

O endereço Classe D: (endereço multicast) - 224.0.0.0 até 239.255.255.255

O endereço Classe E: (endereço especial reservado) - 240.0.0.0 até 247.255.255.254

Endereço reservado

O IANA (Internet Assigned Numbers Authority) é responsável pela coordenação global do DNS raiz, endereçamento IP, o protocolo de Internet e outros recursos.

CIDR - Bloco de Endereços	Descrição
0.0.0.0/8	Rede corrente (só funciona como endereço de origem)
10.0.0.0/8	Rede Privada
14.0.0.0/8	Rede Pública
39.0.0.0/8	Reservado
127.0.0.0/8	Localhost
128.0.0.0/16	Reservado (IANA)
169.254.0.0/16	Zeroconf - APIPA
172.16.0.0/12	Rede Privada
191.255.0.0/16	Reservado (IANA)
192.0.2.0/24	Documentação
192.88.99.0/24	IPv6 para IPv4
192.168.0.0/16	Rede Privada
198.18.0.0/15	Teste de benchmark de redes
223.255.255.0/24	Reservado
224.0.0.0/4	Multicast (rede Classe D)
240.0.0.0/4	Reservado (rede Classe E)
255.255.255.255	Broadcast

Submáscara

O conceito de máscara de endereçamento é uma abordagem existente no protocolo IP com o objetivo de melhoria de desempenho no roteamento dos datagramas. Uma máscara é uma técnica que ajuda a determinar se o endereço de um datagrama é local ou se precisa de um roteamento para uma outra rede. Aplicando um AND lógico com os endereços da máscara e do datagrama, fazemos uma eliminação do endereço de HostId. Em outras palavras, resta apenas o endereço de rede. De posse deste resultado, fica fácil saber se é necessário (ou não) efetuarmos um roteamento do datagrama. A Tabela Abaixo ilustra as classes A, B e C de endereços IPv4 e suas máscaras padrões.

Classe de Endereço	Máscara Padrão (Binária)	Máscara de rede (Decimal)	CIDR
A	11111111.00000000.00000000.00000000	255.0.0.0	/8
B	11111111. 11111111.00000000.00000000	255.255.0.0	/16
C	11111111.11111111. 11111111.00000000	255.255.255.0	/24

Referências bibliográficas

1. SOUZA, Lindeberg Barros de. Redes de Computadores - Guia Total. 1ª ed. São Paulo: Érica,
2. MORAES, Alexandre Fernandes de. Redes de Computadores – Fundamentos. 6ª ed. São Paulo: Érica
3. MARIN, Paulo Sérgio Cabeamento Estruturado - Desvendando cada passo: do projeto à instalação. 3ª ed. São Paulo: Érica
4. DERFLER Jr, Frank J. e Freed, Les. Como Funcionam as Redes III. 4ª ed. São Paulo: Quark Books
5. Wikipédia – A enciclopédia livre - http://pt.wikipedia.org/
6. Professor Jefferson Costa – Educação e tecnologia – http://www.jeffersoncosta.com.br]
7. IEEE - http://www.ieee.org/
8. Viva sem fio - http://www.vivasemfio.com/blog/category/80211_intro/
9. Guia do Hardware - http://www.guiadohardware.net/